

CLAIMS

1. A common key generating method for generating a common key for use in an encryption process of encrypting a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext in cryptographic communication between entities, comprising the steps of:

dividing identification information of one entity into a plurality of blocks to obtain divided identification information;

generating secret keys of the one entity by using the respective divided identification information;

extracting components corresponding to other entity as a communicating party from the generated secret keys of the one entity; and

generating a common key by performing composition of the extracted components after converting the extracted components to increase the number of bits thereof.

2. The common key generating method as set forth in claim 1,

wherein a shift composition is used in performing composition of the extracted components after converting the extracted components to increase the number of bits thereof.

3. A common key generating apparatus, provided for an entity in a cryptographic communication system, for generating a

common key for use in an encryption process of encrypting a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext, comprising

a controller capable of performing the following operations:

(i) extracting, from secret keys of the entity generated using respective divided identification information obtained by dividing identification information of the entity into a plurality of blocks, components corresponding to other entity as a communicating party; and

(ii) generating a common key by performing composition of the extracted components after converting the extracted components to increase the number of bits thereof.

4. The common key generating apparatus as set forth in claim 3,

wherein a shift composition is used in performing composition of the extracted components after converting the extracted components to increase the number of bits thereof.

5. An encryption method for encrypting into a ciphertext a plaintext to be transmitted from a first entity to a second entity, comprising the steps of:

generating secret keys of the first entity by using respective divided identification information obtained by dividing identification information of the first entity into a plurality of

blocks;

generating a common key by extracting components corresponding to the second entity from the generated secret keys and performing composition of the extracted components after converting the extracted components to increase the number of bits thereof; and

encrypting the plaintext into the ciphertext by using the generated common key.

6. A cryptographic communication method for communicating information by a ciphertext between first and second entities, comprising the steps of:

sending secret keys generated using respective divided identification information obtained by dividing identification information of each entity into a plurality of blocks to each of the first and second entities from a plurality of key generating agencies;

at the first entity, generating a first common key by extracting components corresponding to the second entity as a destination of the ciphertext from the respective secret keys of the first entity sent from the respective key generating agencies and performing composition of the extracted components after converting the extracted components to increase the number of bits thereof;

at the first entity, encrypting a plaintext into a ciphertext by using the generated first common key and transmitting the

ciphertext to the second entity;

at the second entity, generating a second common key identical with the first common key by extracting components corresponding to the first entity from the respective secret keys of the second entity sent from the respective key generating agencies and performing composition of the extracted components after converting the extracted components to increase the number of bits thereof; and

at the second entity, decrypting the transmitted ciphertext into a plaintext by using the generated second common key.

7. The cryptographic communication method as set forth in claim 6,

wherein a shift composition is used at the first and second entities in performing composition of the extracted components after converting the extracted components to increase the number of bits thereof.

8. A cryptographic communication system for performing an encryption process of encrypting a plaintext as information to be transmitted into a ciphertext and a decryption process of decrypting the transmitted ciphertext into a plaintext mutually between a plurality of entities, comprising:

a plurality of key generating agencies, each of which generates a secret key of each entity, by using each of respective

divided identification information obtained by dividing identification information of each entity into a plurality of blocks and for transmitting the generated secret key to each entity; and a plurality of entities, each of which generates a common key for use in the encryption process and decryption process by extracting components corresponding to other entity as a communicating party from its own secret keys sent from the key generating agencies and performing composition of the extracted components after converting the extracted components to increase the number of bits thereof.

9. A computer memory product having computer readable program code means for causing a computer to generate a common key for use in an encryption process of encrypting a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext in cryptographic communication between entities, said computer readable program code means comprising:

program code means for causing the computer to extract from secret keys of one entity, which were generated using respective divided identification information obtained by dividing identification information of the one entity into a plurality of blocks, components corresponding to other entity as a communicating party; and

program code means for causing the computer to generate a common key by performing composition of the extracted components

after converting the extracted components to increase the number of bits thereof.

10. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate a common key for use in an encryption process of encrypting a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext in cryptographic communication between entities, comprising:

a code segment for causing the computer to extract from secret keys of one entity, which were generated using respective divided identification information obtained by dividing identification information of the one entity into a plurality of blocks, components corresponding to other entity as a communicating party; and

a code segment for causing the computer to generate a common key by performing composition of the extracted components after converting the extracted components to increase the number of bits thereof.